

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-016596

(43)Date of publication of application : 18.01.2002

(51)Int.Cl.

H04L 9/32
H04N 1/387
H04N 1/44

(21)Application number : 2000-195856

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 29.06.2000

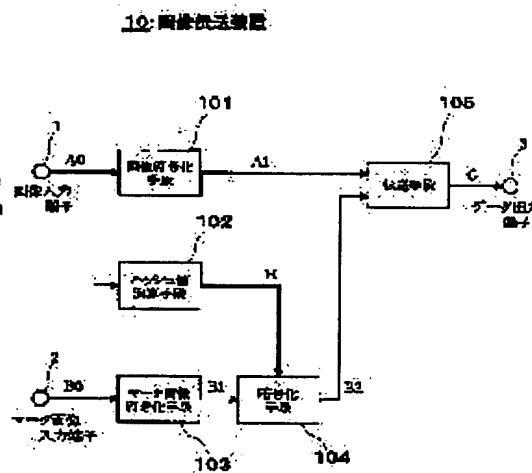
(72)Inventor : MAENO KURATO

(54) IMAGE TRANSMITTER AND IMAGE RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an image transmitter and an image receiver that can easily prevent falsifying of image data and enable the originanness of the image data to be confirmed visually.

SOLUTION: The image receiver 20 receives coded data A1 of an image and coded data B2 of an encrypted mark image that are transmitted from the image transmitter 10 and uses a hash value H of a decoded image A0 for decoding the encrypted mark image. The mark image B0, in combination with the image A0, is outputted. If even part of the image is falsified, the coded data of the mark image which is decoded by using the hash key for a key become one which differ from the coded data that have not been falsified. Thus, viewing the mark image of the image ultimately generated can be confirmed visually and easily as to whether the image has been falsified.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-16596

(P2002-16596A)

(43) 公開日 平成14年1月18日 (2002.1.18)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L 9/32		H 0 4 N 1/387	5 C 0 7 5
H 0 4 N 1/387		1/44	5 C 0 7 6
1/44		H 0 4 L 9/00	6 7 5 A 5 J 1 0 4

審査請求 未請求 請求項の数 6 O L (全 7 頁)

(21) 出願番号 特願2000-195856 (P2000-195856)

(22) 出願日 平成12年6月29日 (2000.6.29)

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 前野 蔵人

東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

(74) 代理人 100095957

弁理士 亀谷 美明 (外3名)

Fターム(参考) 5C075 EE03 EE06

5C076 AA14 AA15 AA19 BA06 BA09

5J104 AA08 LA02 LA05 NA12

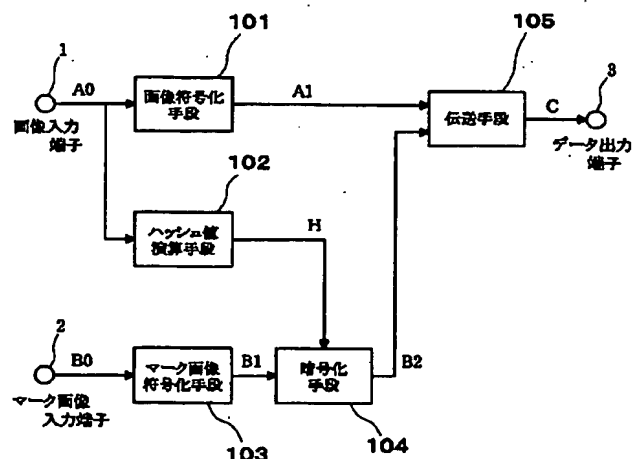
(54) 【発明の名称】 画像伝送装置及び画像受信装置

(57) 【要約】

【課題】 画像データの改竄を容易に防止でき、画像データの原本性を視覚的に確認することの可能な画像伝送装置及び画像受信装置を提供する。

【解決手段】 画像受信装置20は、画像伝送装置10より伝送された、画像の符号化データA1と、暗号化されたマーク画像の符号化データB2とを受信し、復号化された画像A0のハッシュ値Hを用いてマーク画像の暗号解読を行う。マーク画像B0は画像A0と結合されて出力される。画像の一部にでも改竄が行われた場合、そのハッシュ値をキーとして解読されたマーク画像の符号化データは、改竄が行われていない場合の符号化データとは異なったものとなる。このため、最終的に生成される画像のマーク画像を見れば、画像に改竄が行われたか否かを視覚的かつ容易に確認することができる。

10: 画像伝送装置



【特許請求の範囲】

【請求項1】 画像伝送装置において、第1の画像を符号化する第1の画像符号化手段と、前記第1の画像のハッシュ値を計算するハッシュ値演算手段と、第2の画像を符号化する第2の画像符号化手段と、前記第2の画像の符号化データを、前記第1の画像のハッシュ値をキーとして暗号化する暗号化手段と、前記第1の画像の符号化データと前記暗号化された第2の画像の符号化データとを伝送する伝送手段と、を有することを特徴とする、画像伝送装置。

【請求項2】 前記伝送手段は、前記第1の画像の符号化データと前記暗号化された第2の画像の符号化データとを多重化する多重化手段を備えたことを特徴とする、請求項1に記載の画像伝送装置。

【請求項3】 前記第2の画像は、マークを含む印章あるいはサインの画像であることを特徴とする、請求項1または2に記載の画像伝送装置。

【請求項4】 画像受信装置において、第1の画像の符号化データと暗号化された第2の画像の符号化データとを受信する受信手段と、前記第1の画像の符号化データを復号する第1の画像復号化手段と、前記復号された第1の画像のハッシュ値を計算するハッシュ値演算手段と、前記暗号化された第2の画像の符号化データを、前記第1の画像のハッシュ値をキーとして解読する暗号解読手段と、前記解読された第2の画像の符号化データを復号する第2の画像復号化手段と、前記復号された第1の画像と前記復号された第2の画像とを結合する画像結合手段と、を備えたことを特徴とする、画像受信装置。

【請求項5】 前記受信手段は、前記第1の画像の符号化データと前記暗号化された第2の画像の符号化データとが多重化されている場合に、該多重化データを分離する多重化分離手段を備えたことを特徴とする、請求項4に記載の画像受信装置。

【請求項6】 前記第2の画像は、マークを含む印章あるいはサインの画像であることを特徴とする、請求項4または5に記載の画像受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は画像伝送装置及び画像受信装置にかかり、特に、画像データの改竄を防止し、原本性を保証することの可能な画像伝送装置及び画像受信装置に関する。

【0002】

【従来の技術】近年、書類や請求書などを画像データとしてコンピュータに取り込み、電子メールシステムを用いてデータをやり取りするいわゆるペーパーレス対策を講じる企業が増加しつつある。しかしながら、近年におけるコンピュータ関連技術の発達は、かかるペーパーレス対策の一助となる一方で、画像データの容易な改竄をも可能としている。

【0003】従来の紙文化では、書類や請求書に改竄が行われていないこと、すなわち、原本性を保証するために、印章（マークなども含む）やサインなどが用いられていた。また、紙幣や商品券、あるいは公的書面などのように、透かしを用いてその原本性を保証することも行われている。この点、上述のペーパーレス対策を講じるに当たっても、書類や請求書の原本性を保証するための何らかの対策を講じる必要がある。

【0004】画像データの場合、電子的な処理を行えば、視覚的に何ら痕跡を残さずにその一部を改竄することが比較的容易に行える。このため、紙文化の場合のように、単にマークやサインなどを画像データの一部に重ね合わせるのみでは原本性を保証することは難しい。そこで従来より、画像を符号化したデータからハッシュ値を得ることや、画像を符号化したデータに電子透かしを組み込むことで、原本性を保証することが行われている。かかるハッシュ値や電子透かしを用いれば、画像データの一部にでも改竄が行われた場合、画像データの復号の際にその改竄の有無を判断することができる。

【0005】

【発明が解決しようとする課題】ところで、紙文化における印章やサイン、あるいは透かしの場合には、何人もこれを視覚的に確認でき、改竄が行われていないこと（原本性）を容易かつ即座に判断することができる。しかしながら、上述のペーパーレス対策におけるハッシュ値や電子透かしを用いた電子的な処理を用いた場合には、画像データの改竄有無を判断するためには、復号器の操作等の特別な処理が必要であり、容易に判断を行えるものではなかった。

【0006】また、電子透かしを用いた場合、電子透かしを埋め込むアルゴリズムを解析されてしまうと、任意の画像データに対してひとたび画像データを改竄した後に、そのアルゴリズムにより電子透かしを埋め込まれてしまうおそれがある。画像データに電子透かしが埋め込まれているということは、すなわち、その画像データに改竄が行われていないことを保証することであるため、却って、電子透かし技術が画像データの改竄の発見を困難にするという結果となる。

【0007】本発明は、従来の画像データの改竄防止方法が有する上記問題点に鑑みてなされたものであり、本発明の目的は、画像データの改竄を容易に防止でき、画像データの原本性を視覚的に確認することの可能な、新規かつ改良された画像伝送装置及び画像受信装置を提供することである。

【0008】

【課題を解決するための手段】上記課題を解決するため、本発明によれば、請求項1に記載のように、画像伝送装置において、第1の画像を符号化する第1の画像符号化手段と、前記第1の画像のハッシュ値を計算するハッシュ値演算手段と、第2の画像を符号化する第2の画

像符号化手段と、前記第2の画像の符号化データを、前記第1の画像のハッシュ値をキーとして暗号化する暗号化手段と、前記第1の画像の符号化データと前記暗号化された第2の画像の符号化データとを伝送する伝送手段と、を有することを特徴とする、画像伝送装置が提供される。ここで、第2の画像とは、第1の画像の原本性を保証するために用いられる画像であり、例えば、請求項3に記載のように、マークを含む印章あるいはサインの画像である。

【0009】第1の画像の符号化データと暗号化された第2の画像の符号化データは、別々のデータとして伝送するようにしてもよいが、請求項2に記載のように、前記伝送手段に、前記第1の画像の符号化データと前記暗号化された第2の画像の符号化データとを多重化する多重化手段を備えるようにし、多重化データとして伝送することが好ましい。データ伝送の制御を容易に行えとともに、データ量の軽減によるネットワーク資源の軽減を図ることが可能である。

【0010】また、請求項4によれば、画像受信装置において、第1の画像の符号化データと暗号化された第2の画像の符号化データとを受信する受信手段と、前記第1の画像の符号化データを復号する第1の画像復号化手段と、前記復号された第1の画像のハッシュ値を計算するハッシュ値演算手段と、前記暗号化された第2の画像の符号化データを、前記第1の画像のハッシュ値をキーとして解読する暗号解読手段と、前記解読された第2の画像の符号化データを復号する第2の画像復号化手段と、前記復号された第1の画像と前記復号された第2の画像とを結合する画像結合手段と、を備えたことを特徴とする、画像受信装置が提供される。ここで、第2の画像とは、第1の画像の原本性を保証するために用いられる画像であり、例えば、請求項6に記載のように、マークを含む印章あるいはサインの画像である。

【0011】なお、画像の符号化データと暗号化されたマーク画像の符号化データが多重化されたデータとして受信される場合を考慮すると、請求項5に記載のように、前記受信手段に、多重化データを分離する多重化分離手段を備えるようにし、多重化データを受信できる機能を付加することが好ましい。

【0012】かかる画像伝送装置及び画像受信装置によれば、画像の一部にでも改竄が行われた場合、その改竄が行われた画像のハッシュ値は、改竄が行われていない画像のハッシュ値とは異なったものになる。このため、画像の一部にでも改竄が行われた場合、そのハッシュ値をキーとして解読されたマーク画像の符号化データは、改竄が行われていない場合の符号化データとは異なったものとなる。このため、最終的に生成される画像のマーク画像を見れば、画像に改竄が行われたか否かを視覚的かつ容易に確認することができる。

【0013】

【発明の実施の形態】以下に添付図面を参照しながら、本発明にかかる画像伝送装置及び画像受信装置の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。また、以下の説明において、マーク画像とは、印章（マークなどを含む）あるいはサインの画像とする。

【0014】（画像伝送装置10）まず、画像伝送装置の一実施形態を、図1を参照しながら説明する。画像伝送装置10は、図1に示したように、画像A0を符号化する画像符号化手段101と、画像A0のハッシュ値Hを計算するハッシュ値演算手段102と、マーク画像B0を符号化するマーク画像符号化手段103と、マーク画像の符号化データB1を、画像A0のハッシュ値Hをキーとして暗号化する暗号化手段104と、画像の符号化データA1と暗号化されたマーク画像の符号化データB2とを多重化して伝送する多重化手段105とを備えている。

【0015】画像符号化手段101は、画像入力端子1より入力された画像A0を符号化する手段である。ここでの符号化は、JPEG (Joint Photographic Coding Experts Group)、JBIG (Joint Bi-level Image Coding Experts Group)などの、カラー／2値静止画像の符号化の国際標準などが用いられる。

【0016】ハッシュ値演算手段102は、入力された画像A0のハッシュ値Hを計算する手段である。ここでのハッシュ値の演算は、MD5 (Message Digest 5)やDSA (Digital Signature Algorithm)などが用いられる。

【0017】マーク画像符号化手段103は、マーク画像入力端子2より入力されたマーク画像B0を符号化する手段である。ここでの符号化は、画像化符号化手段101と同様に、JPEG、JBIGなどの、カラー／2値静止画像の符号化の国際標準などが用いられる。あるいは、画像伝送装置10内に、一の画像符号化手段のみを備えるように構成し、この一の画像符号化手段により、画像A0及びマーク画像B0の符号化を併せて行うようにしてもよい。

【0018】暗号化手段104は、ハッシュ値演算手段102で得られたハッシュ値Hをキーとして、マーク画像符号化手段103によって符号化されたマーク画像の符号化データB1を、暗号化する。ここでの暗号化は、DES (Data Encryption Standard)やTriple DESなど、共通鍵暗号方式が用いられる。

【0019】伝送手段105では、画像符号化手段101により得られた画像の符号化データA1と、マーク画

像符号化手段 103 により得られた暗号化されたマーク画像の符号化データ B2 の多重化して伝送する。ここでの多重化は、JBIG2 のように、異なる領域の画像データとして多重化する方法や、コメント領域にバイナリデータとして格納する方法などがある。

【0020】なお、本実施の形態では、伝送手段 106 に、データを多重化する機能とデータを伝送する機能とを有する場合について説明するが、データを多重化する機能は必ずしも必須の機能ではなく、画像の符号化データ A1 と、暗号化されたマーク画像の符号化データ B2 とを別のデータとして伝送するようにしてもよい。

【0021】次いで、上述のように構成される画像伝送装置 10 の動作について、データの遷移の観点から、図 2 を参照しつつ説明する。

【0022】画像入力端子 1 より入力された画像 A0 は、ハッシュ値演算手段 102 によってハッシュ値 H が計算されるとともに、画像符号化手段 101 によって符号化される。一方、マーク画像入力端子 2 より入力されたマーク画像 B0 は、マーク画像符号化手段 103 によって符号化される。

【0023】マーク画像符号化手段 103 によって符号化されたマーク画像の符号化データ B1 は、ハッシュ値演算手段 102 で得られたハッシュ値 H をキーとして、暗号化される。

【0024】画像の符号化データ A1 と、暗号化されたマーク画像の符号化データ B2 は、伝送手段 105 によって多重化され、符号化データ C として、データ出力端子 3 より出力される。

【0025】(画像受信装置 20) 次いで、画像受信装置の一実施形態を、図 3 を参照しながら説明する。なお、本実施の形態では、画像受信装置 20 は、上記画像伝送装置 10 が伝送するデータ C を受信するものとして説明する。

【0026】画像受信装置 20 は、図 3 に示したように、画像伝送装置 10 が伝送する符号化データ C を受信し、この符号化データ C を、画像の符号化データ A1 と暗号化されたマーク画像の符号化データ B2 とに分離する受信手段 106 と、画像の符号化データ A1 を復号する画像復号手段 107 と、復号された画像 A0 のハッシュ値 H を計算するハッシュ値演算手段と、暗号化されたマーク画像の符号化データ B2 を、画像 A0 のハッシュ値 H をキーとして解読する暗号解読手段 109 と、解読されたマーク画像の符号化データ B1 を復号するマーク画像復号手段 110 と、復号された画像 A0 と復号されたマーク画像 B0 とを結合する画像結合手段 111 とを備えている。

【0027】受信手段 105 では、画像伝送装置 10 のデータ出力端子 3 より伝送された符号化データ C を受信し、この符号化データ C を、画像の符号化データ A1 と暗号化されたマーク画像の符号化データ B2 とに分離す

る。なお、本実施の形態では、画像受信装置 20 は、多重化された符号化データ C を受信し、この多重化データを分離する機能を有する場合について説明するが、画像の符号化データ A1 と暗号化されたマーク画像の符号化データ B2 とが別のデータとして伝送される場合には、受信手段 105 には、多重化データを分離する機能は必ずしも必須の機能ではない。

【0028】画像復号化手段 107 は、受信手段 106 で得られた画像の符号化データ A1 を復号化する手段である。ここでの復号化は、上記画像伝送装置 10 内の画像符号化手段 101 に対応した機能であるものとし、符号化データ A1 を復号化して画像 A0 を得る。

【0029】ハッシュ値演算手段 108 は、画像復号化手段 107 で得られた画像 A0 のハッシュ値 H を計算する。ここでのハッシュ値の演算は、上記画像伝送装置 10 内のハッシュ値演算手段 102 と同様に、MD5 (Message Digest 5) や DSA (Digital Signature Algorithm) などが用いられる。

【0030】暗号解読手段 109 は、受信手段 106 で得られた暗号化されたマーク画像の符号化データ B2 を、ハッシュ値演算手段 108 より得られたハッシュ値 H をキーとして、解読する。ここでの暗号解読は、上記画像伝送装置 10 内の暗号化手段 104 に対応した機能であるものとし、暗号化されたマーク画像の符号化データ B2 を解読してマーク画像の符号化データ B1 を得る。

【0031】マーク画像復号化手段 110 は、暗号解読手段 109 で得られたマーク画像の符号化データ B1 を復号化する手段である。ここでの復号化は、上記画像伝送装置 10 内のマーク画像符号化手段 103 に対応した機能であるものとし、マーク画像の符号化データ B1 を復号化してマーク画像 B0 を得る。

【0032】画像結合手段 111 は、画像復号化手段 107 で得られた画像 A0 と、マーク画像復号化手段 110 で得られたマーク画像 B0 を結合する手段である。ここでの結合方法は、AND や OR、加算、置換などが用いられる。画像 A0 とマーク画像 B0 が結合され得られた画像 D は、画像出力端子 6 より出力される。

【0033】次いで、上述のように構成される画像受信装置 20 の動作について、データの遷移の観点から、図 4 を参照しつつ説明する。

【0034】データ入力端子 4 より入力されたデータ C は、多重化データの分離機能を有する受信手段 106 によって受信され、画像の符号化データ A1 と、暗号化されたマーク画像の符号化データ B2 とに分離される。

【0035】画像の符号化データ A1 は、画像復号化手段 107 により復号化される。復号化された画像 A0 は、ハッシュ値演算手段 108 によりハッシュ値 H が計算される。

【0036】暗号化されたマーク画像の符号化データB2は、画像A0のハッシュ値Hをキーとして、暗号解読される。暗号解読されたマーク画像の符号化データB1は、マーク画像復号化手段110により、復号化される。

【0037】画像復号化手段107により復号化された画像A0と、マーク画像復号化手段110により復号化されたマーク画像B0は、画像結合手段111によって結合（オーバーレイ、多層化）される。結合された画像Dは、画像出力端子6より出力される。

【0038】図4に示した例では、画像A0に改竄が行われておらず、ハッシュ値Hが正しいものであるため、出力画像Dには、正しいマーク画像が表示されている。画像A0の一部にでも改竄が行われていた場合、ハッシュ値演算の性格上、ハッシュ値演算手段108は異なるハッシュ値H'を算出する。このハッシュ値H'を暗号鍵として解読され、復号化されたマーク画像は、正しいマーク画像B0とは異なった画像（ノイズ）となるか、あるいは復号化が正常に行われず、マーク画像を得ることができない。このようにして、画像の原本性を視覚的かつ容易に確認することができるのである。

【0039】以上説明したように、本実施の形態にかかる画像伝送装置10及び画像受信装置20によれば、画像の一部にでも改竄が行われた場合、その改竄が行われた画像のハッシュ値は、改竄が行われていない画像のハッシュ値Hとは異なったものになる。このため、画像の一部にでも改竄が行われた場合、そのハッシュ値をキーとして解読されたマーク画像の符号化データは、改竄が行われていない場合の符号化データとは異なったものとなる。このため、最終的に生成される画像のマーク画像を見れば、画像に改竄が行われたか否かを視覚的かつ容易に確認することができる。

【0040】以上、添付図面を参照しながら本発明にかかる画像伝送装置及び画像受信装置の好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、特許請求の範囲に記載された技術的思

想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【0041】

【発明の効果】以上説明したように、本発明によれば、画像データの改竄を容易に防止でき、画像データの原本性を視覚的に確認することが可能である。

【図面の簡単な説明】

【図1】画像伝送装置の一実施形態を示す説明図である。

【図2】図1の画像伝送装置におけるデータの遷移を示す説明図である。

【図3】画像受信装置の一実施形態を示す説明図である。

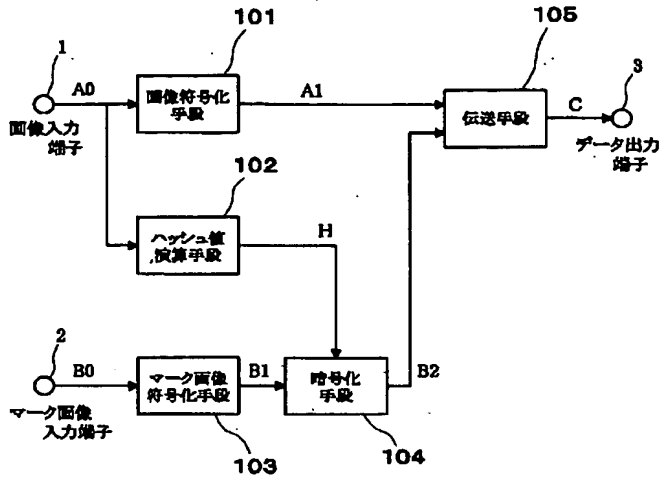
【図4】図3の画像受信装置におけるデータの遷移を示す説明図である。

【符号の説明】

- 10 画像伝送装置
- 1 画像入力端子
- 2 マーク画像入力端子
- 101 画像符号化手段
- 102 ハッシュ値演算手段
- 103 マーク画像符号化手段
- 104 暗号化手段
- 105 伝送手段
- 3 データ出力端子
- 20 画像受信装置
- 4 データ入力端子
- 106 受信手段
- 107 画像符号化手段
- 108 ハッシュ値演算手段
- 109 暗号解読手段
- 110 マーク画像符号化手段
- 111 画像結合手段
- 6 画像出力端子

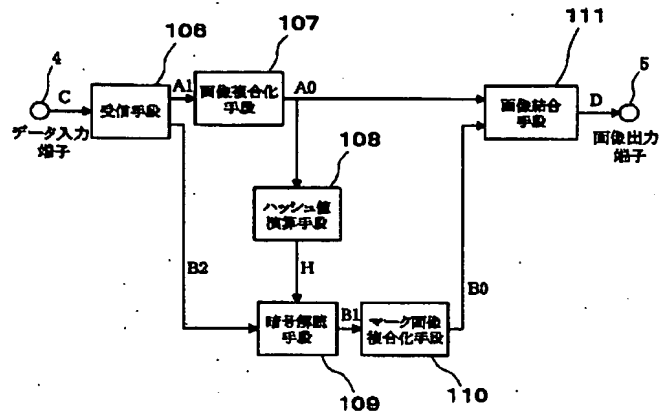
【図 1】

10: 画像伝送装置

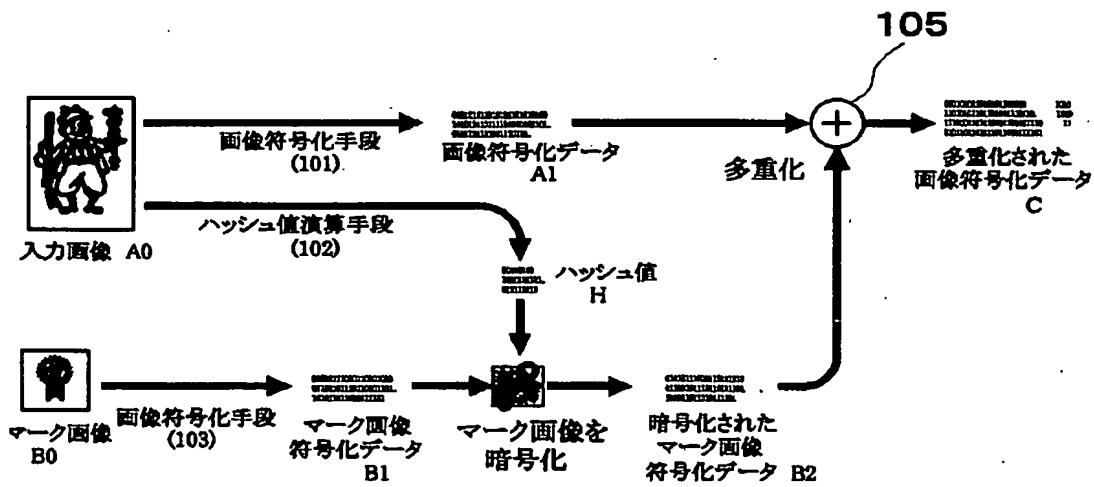


【図 3】

20: 画像受信装置



【図 2】



【図 4】

